

1 CLAIMS

2 1. A session-state management method comprising:
3 generating an encoded session-state token, wherein the token incorporates a
4 representation of session state of a client;
5 encrypting the encoded token using a one-way encryption scheme to
6 produce an encrypted token; and
7 sending the encrypted token to the client.

8
9 2. A method as recited in claim 1, further comprising authenticating the
10 user of the client.

11
12 3. A method as recited in claim 1, further comprising authenticating the
13 user of the client, wherein the authenticating step comprises:

14 receiving a user identification indicator ("username") and a password;
15 comparing the username to a database of authorized user records, each
16 record containing a username and a username-associated password;
17 comparing the password received in the receiving step to a username-
18 associated password of a record containing a matching username; and
19 establishing a session for the user.

20
21 4. A method as recited in claim 1, wherein the generating step
22 comprises forming a confirmation token that incorporates a representation of an
23 incremental time block.
24
25

1 5. A method as recited in claim 1, wherein the generating step
2 comprises forming a confirmation token that incorporates a representation of a
3 current incremental time block.

4
5 6. A method as recited in claim 1, wherein the generating step
6 comprises forming a confirmation token that incorporates a representation of an
7 incremental time block that is prior a current incremental time block.

8
9 7. A computer-readable storage medium having computer-executable
10 instructions that, when executed by a computer, performs the method as recited in
11 claim 1.

12
13 8. A session-state management method comprising:
14 receiving a one-way encrypted, session-state token from a client, wherein
15 the token incorporates a representation of session state of a client;
16 generating a one-way encrypted, confirmation session-state token;
17 comparing the confirmation token with the received token.

18
19 9. A method as recited in claim 8, wherein the generating step
20 comprises forming a confirmation token that incorporates a representation of an
21 incremental time block.

1 **10.** A method as recited in claim 8, wherein the generating step
2 comprises forming a confirmation token that incorporates a representation of a
3 current incremental time block.

4
5 **11.** A method as recited in claim 8, wherein the generating step
6 comprises forming a confirmation token that incorporates a representation of an
7 incremental time block that is prior a current incremental time block.

8
9 **12.** A method as recited in claim 8, further comprising:
10 issuing a one-way encrypted, replacement session-state token;
11 sending the replacement token to the client.

12
13 **13.** A method as recited in claim 12, wherein the issuing step comprises
14 forming a replacement token that incorporates a representation of a current
15 incremental time block.

16
17 **14.** A method as recited in claim 8, wherein the generating step
18 comprises forming a confirmation token that incorporates a representation of an
19 incremental time block, if confirmation and received tokens fail to match, the
20 method further comprising:

21 generating a new one-way encrypted, confirmation session-state token,
22 wherein the confirmation token incorporates a representation of a previous
23 incremental time block;

24 comparing the new confirmation token with the received token.
25

1 15. A method as recited in claim 14, wherein the new-confirmation-
2 token generating step comprises forming a confirmation token that incorporates a
3 representation of an incremental time block, if confirmation and received tokens
4 fail to match, the method further comprising:

5 repeating the steps of new-confirmation-token generating and comparing
6 the new and received tokens, wherein each subsequent reiteration of such steps
7 employs a representation of a previous incremental time block that is previous a
8 previous reiteration of the same steps, for a specified number of times or until
9 compared tokens match.

10
11 16. A computer-readable storage medium having computer-executable
12 instructions that, when executed by a computer, performs the method as recited in
13 claim 8.

14
15 17. A session-state management method comprising:

16 (A) receiving a one-way encrypted, session-state token from a client;

17 (B) generating a one-way encrypted, confirmation session-state token,
18 wherein the confirmation token incorporates a representation of a current
19 incremental time block;

20 (C) comparing the confirmation token with the received token;

21 (D) if the confirmation token and the received token match,

22 (1) issuing a one-way encrypted, replacement session-state token,
23 wherein the replacement token incorporates a representation of a current
24 incremental time block;

25 (2) sending the replacement token to the client.

1 if the confirmation token and the received token fail to match,

2 (3) generating a new one-way encrypted, confirmation session-state
3 token using the one-way encryption scheme of the encryption step,
4 wherein the token incorporates a representation of a previous incremental
5 time block;

6 (4) comparing the new confirmation token with the received token;

7 (5) if the new confirmation and received tokens fail to match, then
8 further comprising:

9 (i) repeating the steps of new-confirmation-token generating
10 and comparing the new and received tokens, wherein each
11 subsequent reiteration of such steps employs a representation of a
12 previous incremental time block that is previous a previous
13 reiteration of the same steps, for a specified number of times;

14 (ii) if, during the repeating step, the confirmation token
15 matches the received token,

16 (a) issuing a one-way encrypted, replacement session-
17 state token, wherein the token incorporates a representation
18 of a current incremental time block;

19 (b) sending the replacement token to the client.

20
21 **18.** A computer-readable storage medium having computer-executable
22 instructions that, when executed by a computer, performs the method as recited in
23 claim 17.
24
25

1 **19.** A session-state management method comprising:
2 authenticating a user of a client to establish a session with the user;
3 generating an encoded session-state token, wherein the encoded token
4 incorporates a representation of session-state of the user's session;
5 sending the session-state token to the client.

6
7 **20.** A method as recited in claim 19, wherein the authenticating step
8 comprises:
9 receiving a user identification indicator ("username") and a password;
10 comparing the username to a database of authorized user records, each
11 record containing a username and a username-associated password;
12 comparing the password received in the receiving step to a username-
13 associated password of a record containing a matching username; and
14 establishing a session for the user.

15
16 **21.** A method as recited in claim 19, wherein:
17 the user is identified by a user identification indicator (UserID);
18 the generating step comprises forming a session-state token at least partially
19 based upon the UserID.

20
21 **22.** A method as recited in claim 19, wherein:
22 a time block is identified by a time block identification indicator (TimeID);
23 the generating step comprises forming a session-state token at least partially
24 based upon the TimeID.
25

1 **23.** A method as recited in claim 19, wherein:
2 the user is identified by a user identification indicator (UserID);
3 a time block is identified by a time block identification indicator (TimeID);
4 the generating step comprises forming a session-state token at least partially
5 based upon the UserID and the TimeID.

6
7 **24.** A method as recited in claim 19, further comprising encrypting the
8 encoded token between the generating and the sending steps.

9
10 **25.** A method as recited in claim 19, further comprising one-way
11 encrypting the encoded token between the generating and the sending steps

12
13 **26.** A method as recited in claim 19, wherein:
14 the user is identified by a user identification indicator (UserID);
15 a time block is identified by a time block identification indicator (TimeID);
16 the generating step comprises combining UserID and TimeID to produce an
17 encoded token.

18
19 **27.** A computer-readable storage medium having computer-executable
20 instructions that, when executed by a computer, performs the method as recited in
21 claim 19.

1 **28.** A session-state token generation method, wherein an authenticated
2 user is identified by a user identification indicator (UserID) and a time block
3 identification indicator (TimeID) identifies a specific time block, the method
4 comprising:

5 combining UserID and TimeID to produce an encoded token;
6 encrypting the encoded token.

7
8 **29.** A method as recited in claim 28, wherein the combining step
9 comprises concatenating UserID and TimeID.

10
11 **30.** A method as recited in claim 28, wherein the combining step
12 comprises concatenating UserID, TimeID, and a code key.

13
14 **31.** A method as recited in claim 28, wherein the encrypting steps
15 comprises encrypting the encoded token using a one-way encryption scheme.

16
17 **32.** A method as recited in claim 28, wherein the encrypting steps
18 comprises:

19 encrypting the encoded token using a one-way encryption scheme to
20 produce an encrypted result; and

21 selecting a defined portion of the encrypted result to form a session-state
22 token.

1 **33.** A computer-readable storage medium having computer-executable
2 instructions that, when executed by a computer, performs the method as recited in
3 claim 28.

4
5 **34.** A session-state management method comprising:
6 receiving a user-associated, encoded session-state token from a client,
7 wherein the encoded token incorporates a representation of session-state of the
8 user's session;
9 generating an encoded, confirmation session-state token;
10 comparing the received token with the confirmation token.

11
12 **35.** A method as recited in claim 34, wherein the generating step
13 comprises forming a confirmation token that incorporates a representation of a
14 current incremental time block, if confirmation and received tokens fail to match,
15 further comprising:

16 generating a new confirmation token using a representation of a
17 incremental time block previous of the time block representation used for the
18 previous generating step;

19 comparing the new confirmation token with the received token.
20
21
22
23
24
25

1 **36.** A method as recited in claim 35, if confirmation and received tokens
2 fail to match, further comprising:

3 repeating the steps of generating a new confirmation token and comparing
4 the new and received tokens, wherein each subsequent reiteration of these steps
5 uses a representation of a previous incremental time block that is previous a
6 previous reiteration of the same steps, for a specified number of times or until
7 compared tokens match.

8
9 **37.** A method as recited in claim 34, wherein the user-associated
10 session-state token is encrypted.

11
12 **38.** A method as recited in claim 34, wherein the user-associated
13 session-state token is one-way encrypted.

14
15 **39.** A computer-readable storage medium having computer-executable
16 instructions that, when executed by a computer, performs the method as recited in
17 claim 34.

18
19 **40.** A session-state management method comprising:
20 receiving a user-associated TimeID from a client, wherein the encoded
21 token incorporates a representation of session-state of the user's session;
22 designating a first time block identification indicator (TimeID) for a first
23 time block;
24 comparing the user-associated TimeID with the first TimeID.
25

1
2 **41.** The method of claim 40, further comprising:
3 designating a prior TimeID for a time block prior to the first time block;
4 comparing the user-associated TimeID with the prior TimeID.

5
6 **42.** A server to communicate with a client over a communications
7 network, the server comprising:

8 a processor;

9 a session-state manager executable on the processor to:

10 generate a session-state token, wherein the token incorporates a
11 representation of session state of the client;

12 encrypt the token using a one-way encryption scheme to produce an
13 encrypted token; and

14 send the encrypted token to the client.

15
16 **43.** A server to communicate with a client over a communications
17 network, the server comprising:

18 a processor;

19 a session-state manager executable on the processor to:

20 receive a one-way encrypted, session-state token from the client,
21 wherein the token incorporates a representation of session state of a client;

22 generate a one-way encrypted, confirmation session-state token;

23 compare the confirmation token and the received token.
24
25

1 **44.** A server to communicate with a client over a communications
2 network, the server comprising:

3 a processor;

4 a session-state manager executable on the processor to:

5 authenticate a user of the client;

6 generate an encoded session-state token, wherein the token
7 incorporates a representation of session state of the client; and

8 send the session-state token to the client.

9
10 **45.** A manager as recited in claim 44, wherein session-state manager
11 executable on the processor to encrypt the encoded session-state token.

12
13 **46.** A manager as recited in claim 44, wherein session-state manager
14 executable on the processor to one-way encrypt the encoded session-state token.

15
16 **47.** A server to communicate with a client over a communications
17 network, wherein an authenticated user is identified by a user identification
18 indicator (UserID) and a time block identification indicator (TimeID) identifies a
19 specific time block, the server comprising:

20 a processor;

21 a session-state manager executable on the processor to:

22 combine UserID and TimeID to produce a encoded token; and

23 encrypt the encoded token.

1 **48.** A server to communicate with a client over a communications
2 network, the server comprising:

3 a processor;

4 a session-state manager executable on the processor to:

5 receive a user-associated, encoded session-state token from the
6 client;

7 generate an encoded, confirmation session-state token, wherein the
8 confirmation token incorporates a representation of session state of the
9 client;

10 compare the received token with the confirmation token.

11
12 **49.** A computer-readable storage medium having computer-executable
13 instructions that, when executed by a computer, performs the method comprising:

14 generating an encoded session-state token, wherein the token incorporates a
15 representation of session state of a client;

16 encrypting the encoded token using a one-way encryption scheme;

17 sending the encrypted token to the client.

18
19 **50.** A computer-readable storage medium having computer-executable
20 instructions that, when executed by a computer, performs the method comprising:

21 receiving a one-way encrypted, session-state token from a client, wherein
22 the token incorporates a representation of session state of a client;

23 generating a one-way encrypted, confirmation session-state token;

24 comparing the confirmation token with the received token.
25